REMARKS

Claims 1-10 are pending in the instant application. Claims 1 has been cancelled and replaced with new claim 11. Support for the new claim is found in claim 1 and in the specification as originally filed on page 3, lines 16-31 and page 4, lines 6-34. No new matter has been added. Claims 2-4 and 9 have been amended; claims 5-8 and 10 were previously amended by a Preliminary Amendment on December 21, 2000. The Abstract has been rewritten to correspond with clarifying changes made in the claims.

Claims 1-7 have been rejected under 35 USC §102(a) as being anticipated by U.S. Patent No. 6,496,928 to Deo et al. (hereinafter Deo).

Deo discloses a method of controlling access to broadcast messages received by a plurality of mobile devices (primarily personal digital assistants) 18. The system comprises providing mobile devices 18 with a broadcast encryption key (BEK) 268 including a group code and encrypting the broadcast messages using the BEK 268 prior to broadcasting the messages such that the mobile devices having the BEK 268 are configured to decrypt the encrypted broadcast messages. The encrypting process further comprises obtaining a message specific broadcast key (MSBK) 296 based on the BEK 268 and message specific data 294, specific to the broadcast message. The broadcast message is encrypted with the MSBK 296 in order to obtain an encrypted broadcast message. Message specific data 294 in unencrypted form and a header 302 is then added to the encrypted broadcast message 300. The resulting completed encrypted broadcast messages 304 are broadcast to the mobile device 18 over an address and the group code associated with the BEK 268. The selected mobile devices 18 are provided with the group code, and the encrypted broadcast message 304 are received on the selected mobile devices 18. The encrypted broadcast messages 304 are decrypted on the selected mobile devices 18 using the BEK 268. The mobile devices in the Deo invention are electronic computing devices often referred to as personal digital assistants. Examples include pagers, hand held devices or palm size devices.

The claims of the instant invention recite a method for signing a message from a sender and for checking a signature at a receiver, in which the method comprises providing a control center, a sender and a receiver. The control center and the receiver share an undiscoverable main key. The control center produces one or more sequence numbers; one of these created sequence numbers are used along with the common undiscoverable main key to produce a signing key by means of a one-time encryption process. The signing key and the sequence number are provided to the sender via a secure transmission and the sender uses the signing key to form a signature for a message. The message is sent to the receiver via a data set containing at least the message and the signature. The receiver determines the sequence number from the received data set and passes the sequence number through a one-time encryption process, which results in the production of a check key. The check key is used to verify the signature on the message.

The undiscoverable main key shared by the control center and the receiver is unique to the instant invention and is not implicitly or explicitly disclosed in Deo. In addition, as described above, the encrypted broadcast message in Deo is generated by different steps than in the instant invention. Furthermore, the problem solved by applicant's invention is to eliminate the sender having to send a message to the control center since the control center cannot provide the sender with the secret main key without weakening the entire system. This aspect is not taught or remotely suggested in Deo. For an anticipation rejection to be appropriate, each and every element or limitation in a rejected claim must be shown in the prior art reference used in the claim rejection. Because Deo does not show or even remotely suggest the characteristic of a one-time encryptor, which is used so that it is virtually impossible to deduce the main key, it can be asserted that claim 1 (which is now new added claim 11) is not anticipated by Deo. Furthermore, as stated by the Federal Circuit "anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim" *W.L Gore & Assoc. v Garlock*, 721 F.2nd 1540, 220 USPQ 303 (Fed. Cir. 1983). The elements of claim 1 and the order in which they are presented are not present in the Deo reference. We respectfully submit that the Examiner has not established a *prima facie* case of anticipation. Deo addresses efficient subscription management, wherein a number of encryption operations must be performed to achieve this objective. Deo does not

disclose a control center having a first memory for a secret key and a receiver containing a corresponding memory, which contains the same key, both of which are elements of the instant invention. In addition, Deo does not disclose or teach the generation of sequence number pairs by a generator in a control center in addition to the main key. Deo does not teach or remotely suggest the production of a signing key provided in advance with the main key to a sender or using generated sequence numbers with the main key to generate a check key to verify the signature of the message in the receiver. Furthermore, because claims 2-7 each depend from and thereby incorporate the limitation of claim 1, claims 2-7 are likewise deemed not anticipated or obvious by Deo for the reasons set forth for claim 1. Therefore, the rejection is traversed and reconsideration is respectfully requested.

Claim 8 has been rejected under 35 USC §103 as being unpatentable over by U.S. Patent No. 6,496,928 to Deo et al. (hereinafter Deo) as applied to claim 8 above, in view of U.S. Patent No. 6,009,401 to Horstmann (hereinafter Horstmann).

Horstmann discloses a mechanism for use in conjunction with Electronic Software Distribution (ESD) that provides purchase documentation and that allows for convenient re-download and relicensing of software, including old software versions. In one embodiment of the invention, a relicensing manager software utility installed on an end user's machine interacts with one or more of a remote publisher site, a license clearing house and a merchant site to relicense, transfer, or obtain a refund for a software product. The role of the license-clearing house is to keep a count of licensed installations and to grant or deny permission to relicense based on the count. The clearinghouse keeps a list of used sequence numbers to avoid a replay attack.

It is respectfully submitted that neither the Deo or Horstmann reference appears to disclose the instant invention in its entirety, either separately or taken together. As to claim 8, there is no teaching or suggestion that the Deo and Horstmann references be combined. The test under section 103 is not whether an improvement or use set forth in a patent would have been obvious or nonobvious; rather the test is whether the claimed invention, considered as a whole, would have been obvious. *Jones v. Hardy*, 110 USPQ 1021, 1024 (Fed. Cir. 1984). Moreover,

the invention as a whole is not restricted to the specific subject matter claimed but embraces its properties and the problem it solves. *In re Wright*, 848 F 2nd 1216, 6 USPQ 1959 (Fed. Cir. 1988). The problem solved by applicant's invention is to eliminate the sender having to send a message to the control center since the control center cannot provide the sender with the secret main key without weakening the entire system. The object of the instant invention is thus to specify a method for corruption protection of messages by means of a signature which can be formed by a sender and can be sent to a receiver without the sender having the secret main key, which is shared by the receiver and a control center, or without the message having to be sent in advance to the control center for signature verification. In contrast, Deo does not teach or remotely suggest this method of corruption protection and Horstmann does not cure this deficiency. Rather, Horstmann merely teaches a method of relicensing electronically purchased software. Accordingly, Deo in view of Horstmann does not render claim 8 obvious. Therefore, the rejection is traversed, and reconsideration is respectfully requested.

Claims 9 and 10 have been rejected under 35 USC § 112, 2nd paragraph, but the Examiner has stated these claims would be allowable if the rejection was appropriately addressed.

The applicant has made clarifying amendments to claims 9 and 10 and, therefore, this rejection is traversed and reconsideration is respectfully requested.

In view of the foregoing, it is respectfully submitted that claims 1-11 are in condition for allowance. All issues raised by the Examiner have been addressed and an early action to that effect is earnestly solicited.

Should any matters remain unresolved, Applicants request that the Examiner contact Applicants representative at the number listed below. While no fees are believed to be due with the filing of this response, Applicants request that any deficiencies in fees be charged to our deposit account number 13-0235.

Respectfully submitted,

By _____

Richard R. Michaud
Registration No. 40,088
Attorney for Applicants

McCormick, Paulding & Huber LLP
CityPlace II
185 Asylum Street
Hartford, Connecticut 06103-3402
(860) 549-5290